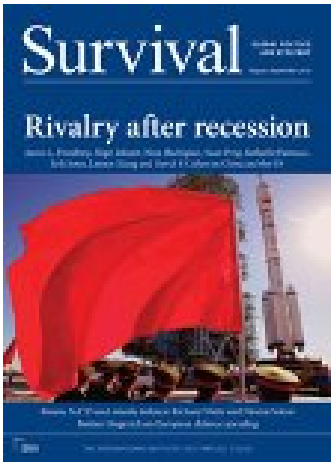

Survival: Global Politics and Strategy
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tsur20

China in Cyberspace

Nigel Inkster

Published online: 21 Jul 2010.

To cite this article: Nigel Inkster (2010) China in Cyberspace, Survival: Global Politics and Strategy, 52:4, 55-66, DOI: 10.1080/00396338.2010.506820

To link to this article: http://dx.doi.org/10.1080/00396338.2010.506820

China in Cyberspace

Nigel Inkster

Over the past four years concern has grown about what is perceived in the West to be an increasingly aggressive cyber threat emanating from China. Awareness of this threat dates back to the early years of the millennium. In 2003 the Pentagon began to register a series of cyber attacks against US government and contractor sites which have collectively been referred to as *Titan Rain*.[1] In 2006–07, a number of Western European governments, including Germany and the UK, publicised the extent to which they too had suffered attacks, with the director-general of the British Security Service taking the unusual step of writing a letter to 300 chief executives and security advisers alerting them to the threat from China.[2] Since then a number of other large-scale cyber-exploitation operations have been reported, amongst them *GhostNet* against the computer networks of the Free Tibet Movement, which involved attacks on over 1,200 computers in 103 countries.[3] In a report prepared in 2009 for the US–China Economic and Security Review Commission, researchers employed by Northrop Grumman list 35 instances of significant Chinese cyber activity against Taiwan and a variety of Western targets between 1999 and 2009.[4]

The overall impression given by this coverage is that China, which now has close to 400 million Internet users, has become something of a cyber superpower. But while it is highly probable that the Chinese state is exploiting Western vulnerabilities in the cyber domain both to collect with minimal

Nigel Inkster is Director of Transnational Threats and Political Risk at the IISS. He served in the British Secret Intelligence Service (SIS) from 1975 to 2006. He is a Chinese speaker and works, inter alia, on China's security and defence policies.

Survival | vol. 52 no. 4 | August–September 2010 | pp. 55–66 DOI 10.1080/00396338.2010.506820

risk valuable scientific, technological and commercial intelligence and to explore weaknesses in military and critical infrastructure systems, this is not a one-way street. Beijing too has considerable anxieties and vulnerabilities with regard to the Internet. It is important for Western policymakers to keep in mind such concerns when dealing with the kinds of threats emanating from China.

The Internet has brought China considerable benefits, as has the introduction of modern PCs and laptops. One look at a traditional Chinese typewriter (essentially a mini-printing press which requires extensive specialist training to use) shows how significant the advent of the modern computer keyboard has been. But the hardware and software which collectively make up the Internet were developed by Western companies with Western users in mind. These systems are not that well suited to the needs of Chinese users. For example, commonly available systems for word processing in Chinese involve typing in Pinyin (the standard form of romanisation for Chinese characters) with the computer offering a menu of characters potentially corresponding to the romanised text in descending order of probability. Since Chinese is a language with many homophones, these menus can be quite long, but predictive software minimises the time spent scrolling through lists. Type in the romanised word *shi* and the Microsoft word-processing system offers a menu of 209 possible characters. But type in *shiqing* – the Chinese word for 'matter, affair' – and the system will offer 事情 as the first and most likely combination.

Most Chinese can type in Pinyin but many find it rather trying. And in recognition of that, indigenous Chinese Internet search engines – Sina, Sohu, Zhongsou and Muzi – are organised very differently from their Western counterparts, with only Baidu offering the kind of portal that would be familiar to users of Western search engines such as Google or Yahoo. The other factor which significantly influences the nature and composition of Chinese search engines is that most Chinese Internet users have different expectations of the Internet from users in the West. A recent study by McKinsey comparing the number of days per week of different forms of Internet usage as between Europe and China demonstrates the extent to which this is the case (Figure 1).

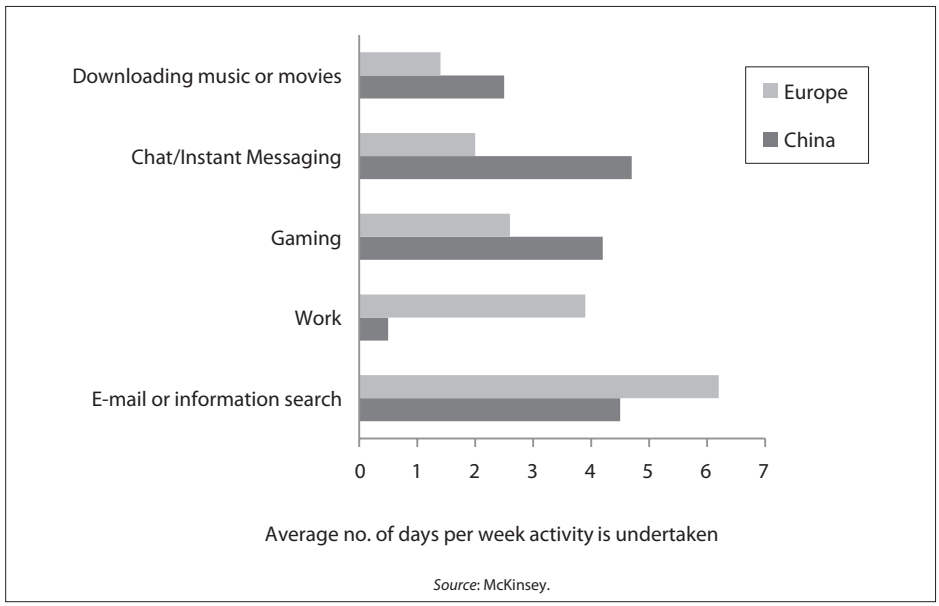

Figure 1. Chinese and European Internet use

These findings tend to confirm that for most Chinese the Internet is a source of recreation and entertainment. And a typical Chinese search engine reflects both this fact and the disinclination of around 70% of Internet users to do much more than navigate around it using mouse clicks. The page from Sina.com reproduced in Figure 2 is typical of what can be found on most Chinese search engines. Information is organised in numerous categories and sub-categories, each of which contains a list of specific articles. There is a space for a free-text search – with Google still offered as the search engine of choice despite uncertainty about whether its licence to operate in China will be renewed – but in the main, the page is organised to provide a very passive experience in which the user selects from a series of prepared options. The fact that majority Chinese preference is for this arrangement may go some way to explaining why Western-style search engines have not gained greater penetration in the Chinese market, other than with the intelligentsia who undoubtedly mourn the departure from China of Google.

One aspect of the Chinese Internet which goes against the general trend of passive usage is the emergence of a lively blogosphere comprising an estimated 50m bloggers, mostly from the better-educated

Figure 2. Chinese search engine homepage

segment of the population which is more comfortable with word-processing in Pinyin.

The organisation of these search engines greatly facilitates, of course, the work of China's large and growing army of Internet censors, who have little difficulty in ensuring that the content of each category on any search engine conforms to what the state thinks its citizens should see. Censorship has been an issue since the arrival of the Internet in China in the mid-1990s. Internet service providers have from the outset been expected to monitor the content of their web pages and blogs, this being one of the issues which led to Google's decision to withdraw from China in March this year. This self-censorship requirement was further enhanced in April 2010 under China's state secrecy laws, with Internet and mobile-phone operators now required to inform the authorities of any illegal information being transmitted on their systems.

In addition to the requirement for service providers to exercise self-censorship, the Chinese state has periodically intervened to close services such as YouTube and Twitter and to remove from the Web content deemed inappropriate. Individual censors also monitor China's blogosphere, often

intervening directly in specific debates to steer them in an 'appropriate' direction or admonish those posting blogs deemed unacceptable. Much of the justification for the state's actions is couched in terms of combating crime and pornography. But while there are periodic crackdowns on sites with sexually explicit content, these are generally short-lived. Not only is there no shortage of pornographic websites available to those wishing to visit them, but sexually explicit advertisements graphically illustrating such things as the benefits of cures for various forms of sexual dysfunction can be found on even the most sober and serious websites. And China's censors appear to have no difficulties with the widespread prevalence of online gaming. Indeed, within the People's Liberation Army (PLA) it is actively encouraged by political commissars who appear to view it as a 'healthy' alternative to visiting foreign news websites.[5]

Crackdowns on sexually explicit sites are generally short-lived

The pervasive nature of censorship might lead outsiders to imagine that the Chinese Internet offers its users a subdued, sterile environment. Nothing could be further from the truth. China's 400m Internet users have adopted a conscious and very deliberate identity as 'netizens' – *wang min* (网民) – which in its collective effect is tantamount to a set of virtual civil-society organisations of the kind not tolerated in the real world of Chinese political life. There have been many instances of the impact produced by on-line campaigns against social injustices, often involving corrupt or authoritarian provincial officials, some of whom have been forced to resign or have been brought to trial as a consequence of the weight of public indignation. A case in point is the cause célèbre of Deng Yujiao, a female hotel employee in Hubei who stabbed to death a senior government official who had attempted to rape her. Following a major popular outcry orchestrated on the Internet, the original charge of murder against Deng was dropped and replaced with a lesser charge of intentional assault. Though found guilty, Deng was not sentenced on the grounds of diminished responsibility. Her assailants were also punished.[6]

The propensity of netizens, in particular those below the age of 30, to take up political causes is something from which the Chinese government

has also sought to benefit. Monitoring China's many blogs offers a convenient means of taking sounding of public opinion, a constant preoccupation of central government officials who take it for granted that their provincial and local counterparts will go to great lengths to conceal the truth from them. And Beijing has found some of the Internet campaigns against malfeasance by provincial and local officials a useful way both of enforcing discipline within a government and party organisation plagued by corruption and gaining a degree of credit when action is seen to be taken against malefactors.

The Chinese government has also sought to leverage the extreme nationalism and sense of historic grievance inculcated in a generation of young Chinese by the Patriotic Education Campaign, conceived in the 1990s to draw attention away from the 'June 4 incident' (the suppression of student demonstrations in Beijing's Tiananmen Square in 1989), by permitting outbreaks of patriotic fervour on the Internet. Such activism has included actions by groups of 'patriotic hackers' to disrupt and deface websites of governments deemed to have incurred China's wrath, as evident following the 2003 collision of a US EP-3 surveillance aircraft with a Chinese fighter jet off the coast of Hainan island, in the reaction to Kofi Annan's suggestion that Japan should be considered for a UN Security Council seat in March 2005, and in the protests in favour of the Free Tibet movement in the run-up to the 2008 Beijing Olympics, the latter resulting in, among other things, a nationwide boycott of the French supermarket chain Carrefour.

Tolerating such behaviour is not without risk, as the Chinese government found when the 2005 anti-Japan protests began to morph into expressions of dissatisfaction with the Chinese government's perceived weakness in dealing with Tokyo. As one blogger put it, 'how can China stand firm when its state leaders are all impotent? If China gives approval this time, the state leaders have no right to sit in their current positions – let them go home and embrace their children.'[7] It appears, however, that Beijing remains confident of its ability to turn off the tap before matters get out of hand.

While China's netizens could not fail to be aware of the phenomenon of censorship they show no signs of being cowed by it, and indeed have developed a vibrant, subversive sub-culture of oblique opposition to censorship.

The following excerpts from a humorous article, which appeared in the *Chongqing Evening News* following Google's announcement of its decision to withdraw from China, is emblematic of this counter-culture:

> The Ancient Dove [*guge* (古鴿) a pun on the Chinese name for Google, 谷歌] is a species of the dove family which, within China's borders, is rapidly moving towards extinction. It is also a kind of private search bird [pun on the Chinese for 'search engine'].
>
> This bird originated in North America with biologists estimating its place of origin as being in the vicinity of the city of Mountain View, Santa Clara County, California. For a period around the turn of the twentieth century it expanded across the planet but after 23 March 2010, this bird began a large-scale migration towards a port off China's southern coast following which it is no longer to be found within China itself.
>
> The best assessment of environmental experts is that the strange behaviour of this bird may be related to recent extremes of climate around the world and in particular to the emergence in China in recent years of ecological, environmental, climatic and geological damage. In the face of difficulties the bird shows none of the resilience of the 'grass mud horse' [*caonima* (草泥马), depicted as a small alpaca-like animal which has achieved iconic status as a symbol of opposition to Internet censorship. It derives from a Chinese homophone, the characters for which are 肏你妈 which translates as 'f*ck your mother'] and simply migrates away, a cause of much sadness to animal lovers.
>
> Initial research suggests that the departure of the Ancient Dove could result in another ferocious species of bird emerging with sharp claws and looking remarkably like the Ancient Dove but with a very different temperament. The Baidu bird [the character used for *du* means 'poison'], this fabled indigenous species, has proliferated drastically and the Chinese population has been left with no option but to resort to this most ferocious of mythical birds which is full of venom and animosity, can only make its call in Chinese and consumes only money, as a substitute for the functions previously provided by the Ancient Dove … The Ancient Dove on the other hand consumes all kinds of printed matter, can independently

> evaluate this material and has complex capacities for cataloguing it. The natural enemy of the Ancient Dove is the river crab [*hexie* (河蟹), which sounds almost the same as the word for 'harmonise', 和谐, a euphemism employed by the censors to describe what they have done to the content of websites].
>
> On the evening of 23 March, many animal lovers gathered at the Ancient Dove Garden in Beijing to take part in mourning ceremonies.

Unsurprisingly, this article disappeared from Chinese search engines within days of publication.

Efforts to impose greater levels of censorship have also encountered more direct and on occasion unexpectedly fierce resistance. In June 2009 the Chinese government announced that in future all PCs sold in China would have to have a pre-installed software filter known as the Green Dam Youth Escort, which would enable the Chinese state to block access to sites with 'unhealthy' content. The declared aim of this exercise was to restrict access to online pornography. In the face of strong objections both from China's netizens and from computer manufacturers including the indigenous Chinese company Lenovo, the Chinese government backed down.[8] It remains to be seen whether further efforts will be made to impose the use of this software which, ironically, is alleged to have been pirated from software developed by the US-based corporation Cybersitter. Cybersitter has since initiated lawsuits against the Chinese government and a number of computer manufacturers in connection with the use of Green Dam.[9]

The fact that China's Internet censors are engaged in constant skirmishing with users who value their intellectual freedom is a symptom of a wider concern affecting a Chinese government which puts political stability above all else. For such a government, the Internet, seen as a quintessentially Western creation, holds many terrors as a vehicle for subversion and the spread of Western ideas and values. Indicative of this view is an op-ed in the *PLA Daily* of 6 August 2009 which makes the following points:

- The West enjoys total dominance over the Internet due to its ownership of the majority of hardware and software.

- It seeks to use the Internet to spread subversion and to promote its own world view.
- The failed colour revolution in Moldova in 2009 was largely instigated via Twitter and Facebook.
- The same was true of the period following Iran's 2009 election when foreign subversion from the Internet gave rise to widespread social unrest.
- After achieving naval, air and space domination, the United States is attempting to achieve dominance in the cyber sphere as evidenced by the creation of a Cyber Command in the Pentagon.
- All of which poses a serious threat to Chinese security.[10]

Similar points were made in a *People's Daily* editorial dated 24 January 2010. More recently, the 29 April 2010 edition of the military newspaper *Jun Bao* carried an article with the characteristically snappy headline 'Our Armed Forces Must Beware of Western Exploitation of the Internet to Undertake Brainwashing'. The article states that the exponents of Westernisation (not further defined) make use of issues such as human rights, democracy and religion to brainwash China's youth. It enjoins China's armed forces to remain alert to the threat, keep a clear head, cultivate good practice on Internet use, avoid actions which break the rules, and refrain from visiting vulgar (*disu*) websites or expressing political views online. In June 2010 the PLA's Political Department issued new instructions prohibiting soldiers from opening blog sites, no doubt in recognition of the fact that such blogs have often been the source of leaks of classified information.

In common with Russia, which has been making this case in discussions with the United States for a number of years, China has begun to talk publicly about the need for international agreement on the policing of cyberspace. Speaking at a conference organised in Dallas, Texas, by the East–West Institute in May 2010, Liu Zhengrong, deputy director-general of the Internet Affairs Bureau of the State Council Information Office, called for international cooperation to safeguard international cyberspace, adding that 'the Internet sovereignty of each country needs to be respected and different national and cultural conditions taken into account'.[11] It is likely

that China will increasingly seek to make common cause with Russia and other like-minded states in forums such as the UN General Assembly. And while any development which risks substituting a series of national intranets for the Internet or otherwise infringes on freedom of expression would be undesirable, there is a legitimate case to be made for some internationally agreed governance of Internet security to deal with issues such as cyber crime and child pornography.

A further concern for China's securocrats is the awareness of their own vulnerability to cyber attack. Whenever allegations of Chinese state-sanctioned cyber-exploitation or hacking operations are made, the default position of Chinese government spokesmen has been to emphasise that China too has been the victim of such operations. Whilst allowing for a certain degree of disingenuousness in such comments, there is more than an element of truth to them. Many Chinese government systems rely on Western hardware and software, much of which is pirated. Such systems do not benefit from the periodic security updates available to purchasers of genuine licensed products and hence over time develop vulnerabilities which can be exploited both by organised criminal groups and by foreign intelligence agencies. The Chinese state has sought to mitigate this risk by promoting 'network sovereignty and indigenous innovation', but continuing demand for Western products suggests that this remains a work in progress. The US National Security Agency in particular benefits from its ability to access the 54% of Internet traffic from Asia which transits the United States.[12] (This is down from 91% in 1994, but still considerable.) And while over time these factors will change in China's favour it is likely to be some while yet before Western dominance of cyberspace will come under serious challenge.

China's securocrats are aware of their own vulnerability to cyber attack

At a time when alarmist press reporting of China's aggressive activity in cyberspace reads like the script of *Mars Attacks!*, it is important to set matters in perspective. Much of China's hostile activity has been made possible by Western governments and corporations who, for many years, have demonstrated remarkable *naiveté* towards the problem of Internet security. Though

such behaviour should not be condoned, it is hardly surprising that China, a still-developing country which has to maintain a very high rate of economic development to meet the demands of a burgeoning workforce, should have harvested so much fruit which is either low-hanging or windfall. Nor is it surprising, given the still substantial disparity between Chinese and US defence capabilities, that China should seek to derive asymmetric advantage from exploiting heavy US military dependence on network-enabled systems. It will be interesting to observe how China's attitude towards this latter issue will evolve as its own military systems and critical national infrastructure become increasingly dependent on network-enabled systems and the improbability of any one nation establishing and maintaining dominance of cyberspace becomes more apparent.

There is much the West can and should do to secure itself against cyber threats from states such as China. An active defence, which combines good defensive security practices with the kind of situational awareness that can only derive from undertaking active cyber-exploitation operations, offers the best way forward. Government in particular has an important role to play. The Internet has developed in the way it has because developers and service providers have, understandably, sought to respond to market demand. And the market has not to date put much of a premium on security. If governments were to send clear signals that security was now an important criterion, security standards could be quickly and significantly enhanced at no great additional cost. China's arrival as a major cyber power is qualitatively no different from its emergence as a major economic or military power and dealing with it will inevitably pose challenges. But these challenges are not insuperable and in addressing them, it would seem sensible neither to overplay the threat it poses nor to overlook its own very real vulnerabilities.

Acknowledgements

The author would like to thank Gary Li for his help in researching this article.

Notes

1 Nathan Thornburgh, 'Inside the Chinese Hack Attack', *Time*, 25 August 2005.

2 David Henvke, 'Whitehall Plans New Cyber Security Centre to Deter Foreign Hackers', *Guardian*, 14 June 2009.

3 Details of an investigation into *GhostNet* undertaken by the Munk Centre and the SecDev Group can be found in the Information Warfare Monitor report of 29 March 2009 entitled *Tracking GhostNet: Investigating a Cyber Espionage Network*, available at http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

4 *Capabilities of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (Washington DC: US–China Economic and Security Review Commission, 2009), pp. 68–74, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved Report_16Oct2009.pdf.

5 'Guofang shengjie wan wangluo youxi zhangwo zhanshu zhishi' [National Defence Makes Use of On-line Gaming to Gain Mastery of Tactical Knowledge], *PLA Daily*, 6 April 2010, available at http://news.xinhuanet.com/mil/2010-04/06/content_13307478.htm.

6 Jane Macartney, 'Waitress Deng Yujiao who Stabbed to Death Communist Official Walks Free', *Times*, 17 June 2009.

7 John Chan, 'Anti-Japanese Protests Erupt in China', World Socialist Web Site, 8 April 2005, http://www.wsws.org/articles/2005/apr2005/chin-a08.shtml.

8 Matthew Taylor, 'China Drops Green Dam Web Filtering System', *Guardian*, 13 August 2009.

9 'US Company Sues China for Green Dam "Code Theft"', BBC News, 6 January 2010, http://news.bbc.co.uk/1/hi/technology/8442771.stm.

10 'Wangluo dianfu: burong xiaoqu de anquan weixie' [Internet Subversion: Not Letting Spies Pose Security Threats], *PLA Daily*, August 2009, available at http://www.chinanews.com.cn/cul/news/2009/08-06/1806701.shtml.

11 Chris Lefkow, 'China Backs International Efforts to Secure Cyberspace', AFP, 3 May 2010, http://www.google.com/hostednews/afp/article/ALeqM5inYEXhRtpODQwIhC7ofP3agm3Jzw.

12 Kelly M. Teal, 'Report: Internet Traffic Flows Beyond US Shores: Changes Part of Web's Natural Evolution, Analysts Say', VON.com, 12 December 2008, http://www.von.com/s.aspx?exp=1&u=http%3A//www.von.com/articles/2008/12/report-internet-traffic-flows-beyond-u-s-shores.aspx.